Realization of positive-operator-valued measures by projective measurements without introducing ancillary dimensions

Guoming Wang[1,*] and Mingsheng Ying[1,†]

[1]State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084

(Dated: February 1, 2008)

We propose a scheme that can realize a class of positive-operator-valued measures (POVMs) by performing a sequence of projective measurements on the original system, in the sense that for an arbitrary input state the probability distribution of the measurement outcomes is faithfully reproduced. A necessary and sufficient condition for a POVM to be realizable in this way is also derived. In contrast to the canonical approach provided by Neumark's theorem, our method has the advantage of requiring no auxiliary system. Moreover, an arbitrary POVM can be realized by utilizing our protocol on an extended space which is formed by adding only a single extra dimension.

PACS numbers: 03.65.Ta, 03.67.-a

Realization of generalized quantum measurements, or positive-operator-valued measures (POVMs), is a fundamental problem in quantum mechanics and quantum information science. Many tasks, such as quantum state discrimination and entanglement transformation, require nonorthogonal measurements to success or to achieve the optimal efficiency. During recent years much effort has been devoted to the implementation of POVMs on various kinds of physical systems [1]. Many of the proposed schemes are derived from Neumark's theorem [2], which asserts that any POVM can be realized by extending the original Hilbert space to a larger space and performing a projective measurement on the extended space. In spite of its universality, this method has the drawback of needing a collective operation on the original system and an ancillary system, which may be difficult to implement in practice.

In this letter, we provide a scheme that can realize a class of POVMs by performing a series of projective measurements on the original system alone, in the sense that for an arbitrary input state the probability distribution of the measurement outcomes is faithfully reproduced. A necessary and sufficient condition for a POVM to be realizable in this way is also derived. Moreover, if only a single ancillary dimension is introduced, then arbitrary POVMs can be realized by applying our protocol on the enlarged space. Nevertheless, our method is limited to the physical systems which can be repeatedly measured, i.e. we have access to the post-measurement states and can perform operations on them again.

Let us begin with the following example. Suppose we are given an arbitrary three-dimensional state, i.e. a qutrit. Consider the following protocol:

(1)Perform the projective measurement $\{|0\rangle\langle 0| + |1\rangle\langle 1|, |2\rangle\langle 2|\}$ on the initial state. Suppose the outcome $r = 0/1$ or 2 is obtained.

(2)If $r = 2$, do nothing. If $r = 0/1$, perform the projective measurement $\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|, |\phi_2\rangle\langle\phi_2|\}$ on the state after stage (1), where $|\phi_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, $|\phi_1\rangle = \frac{1}{\sqrt{14}}(|0\rangle + 2|1\rangle - 3|2\rangle)$, $|\phi_2\rangle = \frac{1}{\sqrt{42}}(5|0\rangle - 4|1\rangle - |2\rangle)$. Suppose the outcome $s = \phi_0$, ϕ_1 or ϕ_2 is obtained.

(3) If $r = 0/1$ and $s = \phi_0$, then output the final outcome 0; if $r = 0/1$ and $s = \phi_1$, then output the final outcome 1; otherwise, output the final outcome 2.

Denoting the initial state by ρ, one can verify that the probabilities of obtaining the final outcomes 0,1 and 2 are $tr(\rho E_0), tr(\rho E_1), tr(\rho E_2)$ respectively, where $E_0 = \frac{2}{3}|\psi_0\rangle\langle\psi_0|$, $E_1 = \frac{5}{14}|\psi_1\rangle\langle\psi_1|$, $E_2 = I - E_0 - E_1$ with $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|\psi_1\rangle = \frac{1}{\sqrt{5}}(|0\rangle + 2|1\rangle)$. Thus, the above protocol actually can be viewed as a 'virtual' POVM $\{E_0, E_1, E_2\}$ if only the measurement outcome is concerned.

The above example demonstrated our basic ideas. Instead of introducing an auxiliary system and performing a collective projective measurement on the extended system, we here repeat projective measurements on the original system over and over again. Suppose we first perform a projective measurement $\{P_1, \ldots, P_m\}$ on the initial state and the outcome i is obtained. Then depending on i we choose another projective measurement $\{P_1^{(i)}, \ldots, P_{m_{(i)}}^{(i)}\}$ and perform it on the state after the first measurement. Suppose its outcome is i_1. Then basing on i and i_1 we construct another projective measurement $\{P_1^{(i,i_1)}, \ldots, P_{m_{(i,i_1)}}^{(i,i_1)}\}$ and perform it on the state after the second measurement. Similarly the protocol goes on. When getting every possible outcome of a performed measurement, we may either to output a final outcome and finish, or to proceed with a new measurement. All these should be specified in advance by the protocol and should not depend on the input state. If such a protocol outputs the final outcomes with the same probability distribution as that of a POVM for an arbitrary input state, we say that this POVM is realized by this protocol, although in our method the final outcome is created more artificially. It is worth noting that every protocol has a concise graphical depiction in the form of a tree structure (For detailed definitions of graphs and trees, see Ref.[3]).

Each leaf node represents a possible outlet of the protocol and has a corresponding final outcome. For the above example, its protocol tree is shown in Fig.1.

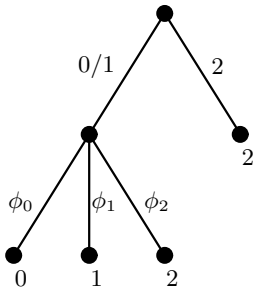

FIG. 1: A graphical depiction of the example protocol. The numbers $0/1, 2$ and symbols ϕ_0, ϕ_1, ϕ_2 along the branches represent the possible outcomes of the measurements. The numbers 0,1 and 2 beside the leaf nodes indicate the final outcomes inferred from the corresponding chain of measurements.

In general, we can come up with much more complex protocols than the one given above. It is easy to observe that any such protocol will generate a POVM. Conversely, we may ask whether an arbitrary POVM can be realized in this way. To understand the limit of our method, suppose that a POVM $\{E_1, \ldots, E_m\}$ is realized by a protocol which begins with a projective measurement $\{P_1, \ldots, P_n\}$. No matter how the protocol works specifically in the subsequent steps, it is always true that every POVM element E_k should be written as the sum of some items $M^\dagger M$ where

$$M = P_{i_t}^{(i,i_1,\ldots,i_{t-1})} \ldots P_{i_2}^{(i,i_1)} P_{i_1}^{(i)} P_i \tag{1}$$

is the product of the projection operators in a chain of measurements. Then we have $M^\dagger M = P_i \Pi P_i$ for some positive operator Π. Thus, E_k could be written in the form $E_k = \sum_{i=1}^n P_i \Omega_{ki} P_i$ for some positive operators Ω_{ki}. It then follows that

$$E_k = \sum_{i=1}^{n} P_i E_k P_i. \tag{2}$$

As a consequence, for each E_k and each P_i, we have $[E_k, P_i] = 0$. So a necessary condition for a POVM to be realizable by our approach is that there exists at least one projection operator $P \neq I$ such that P commutes with all the POVM elements.

Next we will prove that the above condition is also sufficient. Suppose a POVM $\{E_1, ..., E_m\}$ and a projection operator $P \neq I$ satisfy that $[E_i, P] = 0$ for $i = 1, \ldots, m$. Let $E_{i0} = PE_iP$, $E_{i1} = (I - P)E_i(I - P)$, and suppose they have spectral decompositions

$$E_{ia} = \sum_{j=1}^{d_{ia}} \lambda_{ia}^j |\phi_{ia}^j\rangle\langle\phi_{ia}^j|, \tag{3}$$

where $a = 0, 1$, $i = 1, \ldots, m$ and $d_{ia} = rank(E_{ia})$. One can verify that $E_i = E_{i0} + E_{i1}$, $\sum_{i=1}^m E_{i0} = P$ and $\sum_{i=1}^m E_{i1} = I - P$.

Before presenting our protocol for realizing this POVM, a lemma should be stated first:

Lemma 1 *If a linear operator M, a state $|\phi\rangle$ and a number $\lambda > 0$ satisfy $M^\dagger M - \lambda|\phi\rangle\langle\phi| \geq 0$, then there exist a state $|\theta\rangle$ and a number $\mu \geq \lambda$ such that*

$$M^\dagger|\theta\rangle = \sqrt{\mu}|\phi\rangle. \tag{4}$$

Proof. The proof is given in the appendix. □

The constructive proof of this lemma gives us a basic function which takes M, λ and $|\phi\rangle$ as input and outputs μ, $|\theta\rangle$ in the Eq.(4). We write it in the form

$$f(M, \lambda, |\phi\rangle) = (\mu, |\theta\rangle). \tag{5}$$

Our protocol is as follows:

Stage 1: Perform the projective measurement $\{P, I - P\}$ on the initial state. If the outcome corresponding to P is obtained, set $a = 0$; otherwise, set $a = 1$.

Stage 2:

(2.1) Set $i = 1$, $j = 1$. If $a = 0$, set $M_{10}^1 = P$; otherwise, set $M_{11}^1 = I - P$.

(2.2) Compute the function

$$f(M_{ia}^j, \lambda_{ia}^j, |\phi_{ia}^j\rangle) = (\mu_{ia}^j, |\theta_{ia}^j\rangle). \tag{6}$$

(2.3) Choose a state $|\xi_{ia}^j\rangle \in ker(M_{ia}^{j\dagger})$. (This is always possible, and we will prove it later.)

(2.4) Perform the projective measurement $\{|\psi_{ia}^j\rangle\langle\psi_{ia}^j|, I - |\psi_{ia}^j\rangle\langle\psi_{ia}^j|\}$ on the current state, where

$$|\psi_{ia}^j\rangle = \sqrt{\frac{\lambda_{ia}^j}{\mu_{ia}^j}}|\theta_{ia}^j\rangle + \sqrt{1 - \frac{\lambda_{ia}^j}{\mu_{ia}^j}}|\xi_{ia}^j\rangle. \tag{7}$$

If the outcome corresponding to $|\psi_{ia}^j\rangle$ is obtained, then output the final outcome i and exit; otherwise, goto stage (2.5).

(2.5)If $j < d_{ia}$, then set

$$M_{ia}^{j+1} = (I - |\psi_{ia}^j\rangle\langle\psi_{ia}^j|)M_{ia}^j, \tag{8}$$

and increase j by 1; otherwise, set

$$M_{(i+1)a}^1 = (I - |\psi_{ia}^j\rangle\langle\psi_{ia}^j|)M_{ia}^j, \tag{9}$$

increase i by 1, and set $j = 1$.

(2.6)If $i = m$, then output the final outcome m and exit; otherwise goto stage (2.2).

The protocol can be depicted by the tree shown in Fig.2. One can see that its structure is really simple.

To prove the validity of the protocol, it suffices to consider pure input states since the probability of obtaining

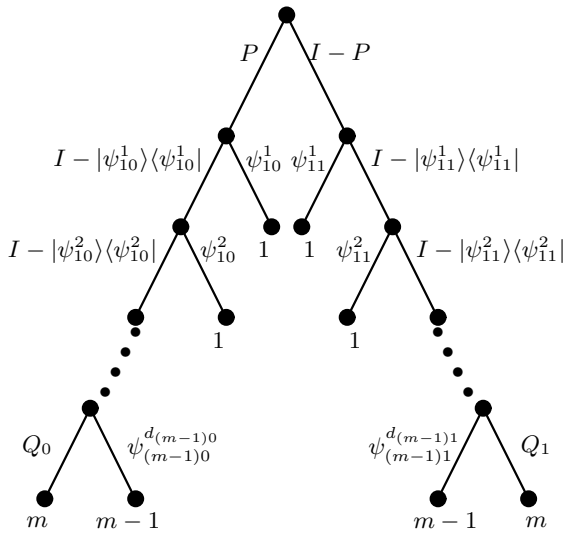

FIG. 2: A graphical depiction of the general protocol. The dotted lines stand for omitted branches. For the measurement outcome corresponding to the state $|\psi_{ia}^j\rangle$ at every iteration of stage (2.4), the symbol ψ_{ia}^j is put along the branch; and for the other outcome, we put the performed linear operation $I - |\psi_{ia}^j\rangle\langle\psi_{ia}^j|$ along the other branch, including $Q_a = I - |\psi_{(m-1)a}^{d_{(m-1)a}}\rangle\langle\psi_{(m-1)a}^{d_{(m-1)a}}|$ where $a = 0, 1$. The numbers 1,...,$m-1$ and m beside the leaf nodes indicate the final outcomes inferred from the corresponding chain of measurements.

each measurement outcome is linear in the density matrix of the input state. Suppose the input state is $|\psi\rangle$. It can be observed that the role of M_{ia}^j is to record the total operation performed on the input state, which means, no matter at what stage of the protocol, the current state is always $|\psi'\rangle = M_{ia}^j|\psi\rangle/\|M_{ia}^j|\psi\rangle\|$ and the protocol can reach this stage with probability $\|M_{ia}^j|\psi\rangle\|^2$.

Since every M_{ia}^j is the product of a chain of projection operators which start with either P or $I - P$, we have $rank(M_{ia}^j) \leq rank(P)$ or $rank(M_{ia}^j) \leq rank(I - P)$, which implies $ker(M_{ia}^{j\dagger}) \neq \emptyset$. So at stage (2.3) the state $|\xi_{ia}^j\rangle$ can always be found.

Consider an arbitrary iteration of stage 2 with $i < m$. First, it is necessary to prove that M_{ia}^j, λ_{ia}^j, and $|\phi_{ia}^j\rangle$ satisfy the condition

$$M_{ia}^{j\dagger}M_{ia}^j - \lambda_{ia}^j|\phi_{ia}^j\rangle\langle\phi_{ia}^j| \geq 0 \tag{10}$$

so that the function f can be applied to them at stage (2.2). This will be proved later. Now we assume that it holds and then by Eq.(4) get

$$M_{ia}^{j\dagger}|\theta_{ia}^j\rangle = \sqrt{\mu_{ia}^j}|\phi_{ia}^j\rangle. \tag{11}$$

By Eq.(7), Eq.(11) and $M_{ia}^{j\dagger}|\xi_{ia}^j\rangle = 0$ we have

$$M_{ia}^{j\dagger}|\psi_{ia}^j\rangle\langle\psi_{ia}^j|M_{ia}^j = \lambda_{ia}^j|\phi_{ia}^j\rangle\langle\phi_{ia}^j|. \tag{12}$$

Then it follows that the probability of obtaining the measurement outcome corresponding to $|\psi_{ia}^j\rangle$ is

$$\begin{aligned}&|\langle\psi_{ia}^j|\psi'\rangle|^2 = \langle\psi|M_{ia}^{j\dagger}|\psi_{ia}^j\rangle\langle\psi_{ia}^j|M_{ia}^j|\psi\rangle/\|M_{ia}^j|\psi\rangle\|^2\\ &= \lambda_{ia}^j\langle\psi|\phi_{ia}^j\rangle\langle\phi_{ia}^j|\psi\rangle/\|M_{ia}^j|\psi\rangle\|^2.\end{aligned} \tag{13}$$

Taking into account the prior probability of reaching this stage $\|M_{ia}^j|\psi\rangle\|^2$, the probability of the protocol stopping at stage (2.4) with the current values of i, j and a is $\lambda_{ia}^j\langle\psi|\phi_{ia}^j\rangle\langle\phi_{ia}^j|\psi\rangle$.

Therefore, the total probability of the protocol yielding the final outcome i is

$$\sum_{a=0}^{1}\sum_{j=1}^{d_{ia}}\lambda_{ia}^j\langle\psi|\phi_{ia}^j\rangle\langle\phi_{ia}^j|\psi\rangle = \sum_{a=0}^{1}\langle\psi|E_{ia}|\psi\rangle = \langle\psi|E_i|\psi\rangle \tag{14}$$

for all $i < m$. And naturally the probability of yielding the final outcome m will be $1 - \sum_{i=1}^{m-1}\langle\psi|E_i|\psi\rangle = \langle\psi|E_m|\psi\rangle$. So this protocol realizes the POVM $\{E_1, \ldots, E_m\}$.

Now we go back to prove that the condition (10) is always fulfilled when $i < m$. Actually, if

$$M_{ia}^{j\dagger}M_{ia}^j = \sum_{j'=j}^{d_{ia}}\lambda_{ia}^{j'}|\phi_{ia}^{j'}\rangle\langle\phi_{ia}^{j'}| + \sum_{i'=i+1}^{m}\sum_{j'=1}^{d_{i'a}}\lambda_{i'a}^{j'}|\phi_{i'a}^{j'}\rangle\langle\phi_{i'a}^{j'}| \tag{15}$$

holds, then the inequality (10) will be true.

We will prove Eq.(15) by induction on the indices (i, j). We consider only the case of $a = 0$, because the case of $a = 1$ can be dealt similarly. At the beginning, $(i, j) = (1, 1)$, $M_{10}^1 = P$. It follows from Eq.(3) and $\sum_{i=1}^m E_{i0} = P$ that

$$\sum_{i=1}^{m}\sum_{j=1}^{d_{i0}}\lambda_{i0}^j|\phi_{i0}^j\rangle\langle\phi_{i0}^j| = P. \tag{16}$$

So Eq.(15) holds. Now suppose that for some indices (i, j), Eq.(15) is valid. If $j < d_{i0}$, then by Eq.(8) and Eq.(12) we have

$$\begin{aligned}&M_{i0}^{(j+1)\dagger}M_{i0}^{j+1} = M_{i0}^{j\dagger}M_{i0}^j - M_{i0}^{j\dagger}|\psi_{i0}^j\rangle\langle\psi_{i0}^j|M_{i0}^j\\ &= \sum_{j'=j+1}^{d_{i0}}\lambda_{i0}^{j'}|\phi_{i0}^{j'}\rangle\langle\phi_{i0}^{j'}| + \sum_{i'=i+1}^{m}\sum_{j'=1}^{d_{i'0}}\lambda_{i'0}^{j'}|\phi_{i'0}^{j'}\rangle\langle\phi_{i'0}^{j'}|,\end{aligned} \tag{17}$$

which implies that Eq.(15) is also valid for the next indices $(i, j+1)$. Similarly, if $j = d_{i0}$, then by Eq.(9) and Eq.(12) the validity of Eq.(15) for the next indices $(i+1, 1)$ can be proved.

To analyze the efficiency of our protocol, we should be aware that its basic idea is to individually realize each item $\lambda_{ia}^j|\phi_{ia}^j\rangle\langle\phi_{ia}^j|$ in Eq.(3) and contribute it to the corresponding POVM element E_i for all $i < m$, while leaving

the residual probability to E_m. Since each item needs exactly a projective measurement, our protocol performs at most $\max_{a=0,1}\{\sum_{i=1}^{m-1} rank(E_{ia})+1\}$ projective measurements in total. Actually we can rearrange the POVM elements $\{E_1,\ldots,E_m\}$ to minimize this upper bound.

Summarizing, we get the following theorem:

Theorem 1 *A POVM $\{E_1,...,E_m\}$ can be realized by a sequence of projective measurements on the original space if and only if there exists a projection operator $P\neq I$ such that $[E_i,P]=0$ for $i=1,\ldots,m$.*

As an application, we consider the problem of unambiguous discrimination [4] of mixed quantum states. Suppose a state is secretly chosen from two quantum states ρ_1 and ρ_2 whose supports have nonempty intersection, i.e. $supp(\rho_1)\cap supp(\rho_2)\neq\emptyset$. Choose a state $|\psi\rangle\in supp(\rho_1)\cap supp(\rho_2)$. If a POVM $\{E_0,E_1,E_2\}$ can be used to unambiguously distinguish the two states (where E_1, E_2 correspond to ρ_1, ρ_2 respectively, and E_0 leads to no conclusion), the condition

$$tr(E_1\rho_2)=tr(E_2\rho_1)=0 \tag{18}$$

should be fulfilled. Then we have $supp(\rho_2)\subset ker(E_1)$ and $supp(\rho_1)\subset ker(E_2)$, which implies $|\psi\rangle\in ker(E_1)$ and $|\psi\rangle\in ker(E_2)$. Let $P=|\psi\rangle\langle\psi|$. Then one can verify that $[E_i,P]=0$ for $i=0,1,2$. Hence this POVM can be realized by our approach.

A surprising consequence of theorem 1 is that when allowing sequences of projective measurements, an arbitrary POVM can be realized by introducing only a single ancillary dimension, as the following corollary states:

Corollary 1 *An arbitrary POVM on a d-dimensional space can be realized by a sequence of projective measurements on an extended $(d+1)$-dimensional space.*

To prove this, note that a POVM $\{E_1,\ldots,E_m\}$ on a d-dimensional Hilbert space $\mathcal{H}$ can be mapped to the POVM $\{E_1,\ldots,E_m,|\psi\rangle\langle\psi|\}$ on any $(d+1)$-dimensional space $\mathcal{H}'$ formed by adding an extra basis element $|\psi\rangle$ to $\mathcal{H}$. Letting $P=|\psi\rangle\langle\psi|$, one can find that our condition holds trivially. So we can realize this POVM by utilizing our protocol on the extended space $\mathcal{H}'$. Note that in this situation, one never needs to perform the projective measurement $\{P,I-P\}$ at stage 1, since only the outcome corresponding to $I-P$ can be obtained. We can directly set $a=1$. The other part of the protocol remains the same.

In conclusion, we present a protocol that can realize a class of POVMs by performing a series of projective measurements on the original system, in the sense that it can simulate the probability distribution of the measurement outcomes for any input state. A necessary and sufficient condition for a POVM to be realizable in this way is also derived. Our method requires no auxiliary system and thus may be easier to implement in practice than the one provided by Neumark's theorem. Moreover, arbitrary POVMs can be realized by adopting our protocol on an extended space which is formed by introducing only a single extra dimension. Our work may help with the implementation of generalized quantum measurements in the tasks where only the measurement outcome is concerned such as quantum state estimation and discrimination.

We gratefully thank Michael Hall for suggesting the elegant expression of our theorem using the Lie bracket [,] and also pointing out corollary 1. This work was supported by the Natural Science Foundation of China (Grants Nos. 60503001, 60321002 and 60305005).

Appendix: Here we prove lemma 1. Suppose M has singular value decomposition $M=\sum_{i=1}^{d}p_i|\psi_i\rangle\langle\phi_i|$, where $p_i>0$, $\langle\psi_i|\psi_j\rangle=\delta_{ij}$, $\langle\phi_i|\phi_j\rangle=\delta_{ij}$, and $d=rank(M)$. Then we have $M^\dagger M$ has spectral decomposition $M^\dagger M=\sum_{i=1}^{d}p_i^2|\phi_i\rangle\langle\phi_i|$. By $M^\dagger M-\lambda|\phi\rangle\langle\phi|\geq 0$, we suppose $M^\dagger M$ can also be written in the form $M^\dagger M=\lambda|\phi\rangle\langle\phi|+\sum_{i=1}^{m}q_i|\zeta_i\rangle\langle\zeta_i|$ for some $m\geq d-1$, $q_i>0$ and $|\zeta_j\rangle$. Then by theorem 2.6 of Ref.[5], we conclude that there exists a $(m+1)\times(m+1)$ unitary matrix $U=(u_{ij})_{i,j=1,\ldots,m+1}$ such that $\sqrt{\lambda}|\phi\rangle=\sum_{i=1}^{d}u_{1i}p_i|\phi_i\rangle$, where $\|u\|^2=\sum_{i=1}^{d}|u_{1i}|^2\leq 1$. Let $|\theta\rangle=\frac{1}{\|u\|}\sum_{i=1}^{d}u_{1i}|\psi_i\rangle$, $\mu=\lambda/\|u\|^2\geq\lambda$. Then we obtain $M^\dagger|\theta\rangle=\frac{1}{\|u\|}\sum_{i=1}^{d}u_{1i}p_i|\phi_i\rangle=\sqrt{\mu}|\phi\rangle$. □

* Electronic address: wgm00@mails.tsinghua.edu.cn
† Electronic address: yingmsh@tsinghua.edu.cn

[1] E. Andersson, Phys. Rev. A **64**, 032303 (2001); S. Franke-Arnold, E. Andersson, S. M. Barnett and S. Stenholm Phys. Rev. A **63**, 052301 (2001); J. Calsamiglia, Phys. Rev. A **65**, 030301(R) (2002); S. Virmani and M. B. Plenio, Phys. Rev. A **67**, 062308 (2003); M. Roško, V. Bužek, P. R. Chouha, and M. Hillery, Phys. Rev. A **68**, 062302 (2003); T. Decker, D. Janzing and M. Rötteler, quant-ph/0407054; S. E. Ahnert and M. C. Payne, Phys. Rev. A **71**, 012330 (2005); M. Ziman and V. Bužek, Phys. Rev. A **72**, 022343 (2005); S. E. Ahnert and M. C. Payne, Phys. Rev. A **73**, 022333 (2006).

[2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, The Netherlands, 1993).

[3] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms (Second Edition)* (MIT Press, 2001).

[4] I. D. Ivanovic, Phys. Lett. A **123,** 257 (1987); D. Dieks, Phys. Lett. A **126,** 303 (1988); A. Peres, Phys. Lett. A **128,** 19 (1988).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000), p.103.